HTTP and HTTPS: What do they do, and how are they different?

You click to check out at an online merchant. Suddenly your browser address bar says **HTTPS** instead of HTTP. What's going on? Is your credit card information safe?

Good news. Your information is safe. The website you are working with has made sure that no one can steal your information.

Instead of HyperText Transfer Protocol (HTTP), this website uses **HyperText Transfer Protocol Secure (**[**HTTPS**](https://www.instantssl.com/ssl-certificate-products/https.html?key5sk1=01e337a5aed0fe185f2ac782f79c9e791ccf2bb1)**)**.

Using HTTPS, the computers agree on a "code" between them, and then they scramble the messages using that "code" so that no one in between can read them. This keeps your information safe from hackers.

They use the "code" on a **Secure Sockets Layer (SSL)**, sometimes called Transport Layer Security (TLS) to send the information back and forth.

How does HTTP work? How is *HTTPS* different from HTTP? This tutorial will teach you about SSL, HTTP and HTTPS.

How Does HTTP Work?

In the beginning, network administrators had to figure out how to share the information they put out on the Internet.

They agreed on a procedure for exchanging information and called it Hypertext Transfer Protocol (HTTP).

Once everyone knew how to exchange information, intercepting on the Internet was not difficult. So knowledgeable administrators agreed upon a procedure to protect the information they exchanged. The protection relies on SSL Certificate to encrypt the online data. Encryption means that the sender and recipient agree upon a "code" and translate their documents into random-looking character strings.

The procedure for encrypting information and then exchanging it is called Hypertext Transfer Protocol Secure (HTTPS).

With **HTTPS** if anyone in between the sender and the recipient could open the message, they still could not understand it. Only the sender and the recipient, who know the "code," can decipher the message.

Humans could encode their own documents, but computers do it faster and more efficiently. To do this, the computer at each end uses a document called an "SSL Certificate" containing character strings that are the keys to their secret "codes."

SSL certificates contain the computer owner's "public key."

The owner shares the public key with anyone who needs it. Other users need the public key to encrypt messages to the owner. The owner sends those users the SSL certificate, which contains the public key. The owner does not share the private key with anyone.

The security during the transfer is called the Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

The procedure for exchanging public keys using [SSL Certificate](https://www.instantssl.com/ssl-certificate.html?key5sk1=01e337a5aed0fe185f2ac782f79c9e791ccf2bb1) to enable HTTPS, SSL and TLS is called Public Key Infrastructure (PKI).